

20-MJ-6557-MPK
20-MJ-6560-MPK

**AFFIDAVIT OF SPECIAL AGENT TIMOTHY TABER IN SUPPORT OF
APPLICATIONS FOR A CRIMINAL COMPLAINT AND A SEARCH WARRANT**

1. I am a Special Agent (“SA”) with the United States Department of Homeland Security, Homeland Security Investigations (“HSI”), and have been so since May 2018. I have received formal training in conducting criminal investigations at the Federal Law Enforcement Training Center in Glynco, Georgia. Prior to becoming a SA with HSI, I was an Intelligence Analyst with the Federal Bureau of Investigation for approximately ten years. I am currently assigned to the HSI Boston, Massachusetts Document and Benefit Fraud Task Force (“DBFTF”), which is comprised of law enforcement agents and officers from federal, state, and local agencies. As part of the DBFTF, I am responsible for conducting investigations involving but not limited to the manufacturing, counterfeiting, alteration, sale, and use of identity documents and other fraudulent documents to evade immigration laws or for other criminal activity. Due to my training and experience, as well as conversations with other law enforcement officers, I am familiar with the methods, routines, and practices of document counterfeiters, vendors, and persons who fraudulently obtain or assume false identities.

2. The DBFTF is currently investigating a group of suspects who are believed to have obtained stolen identities of other United States citizens from Puerto Rico. Many of these individuals used the stolen identities to open bank accounts and/or credit cards to fraudulently purchase, register, and/or export vehicles as part of a multi-state scheme involving financial fraud, auto theft, and the exportation of stolen goods.

3. I am submitting this affidavit in support a criminal complaint charging Alvin RIVERA (“RIVERA”), DOB xx-xx-1983, with false representation of a social security number,

in violation of 42 U.S.C. § 408(a)(7)(B), and aiding and abetting the same, in violation of 18 U.S.C. § 2; aggravated identity theft, in violation of 18 U.S.C. § 1028A, and aiding and abetting the same, in violation of 18 U.S.C. § 2; and wire fraud, in violation of 18 U.S.C. § 1343.

4. I also submit this affidavit in support of an application for a search warrant for the following property: 15 Brockton Avenue, Haverhill, Massachusetts, as described in Attachment A. I have probable cause to believe that this property contains evidence, fruits, and instrumentalities of the crimes identified above, as described in Attachment B.

5. The facts in this affidavit come from my personal involvement in this investigation, including interviews of witnesses, as well as my conversations with other members of law enforcement and my review of documents and bank records. In submitting this affidavit, I have not included every fact known to me about this investigation. Instead, I have only included facts that I believe are sufficient to establish probable cause.

Background of Investigation

6. Since approximately January 2019, HSI special agents have been investigating a scheme involving the use of stolen identities to fraudulently open bank accounts, obtain credit cards, and purchase vehicles, many of which are then exported out of the United States. More specifically, the investigation has revealed a number of individuals using the stolen identities of United States citizens from Puerto Rico to fraudulently finance late-model vehicles from dealerships in Massachusetts, paying zero dollars down. At the dealerships, the individuals provide a variety of fraudulent identification and credit-related documents, including fraudulent Puerto Rico driver's licenses and social security cards as proof of identification. The perpetrators of this fraudulent scheme typically do not make payments on the vehicles, resulting in the dealership or relevant lending financial institution taking a total loss for the vehicles. The

individuals have also been successful in opening bank accounts in the same stolen identities prior to fraudulently purchasing the vehicles. Individuals perpetrating the scheme max out associated credit cards within days or weeks and rarely make any payments on the accounts.

Probable Cause

Fraudulent Vehicle Purchase in Everett by Andy MAZARA

7. On or about October 13, 2018,¹ a man appeared in person at a car dealership in Everett, Massachusetts (the “Everett Dealership”), and provided personal identifying information on a credit application in an attempt to purchase a 2016 Honda Accord S (VIN: XXXXXXXXXXXXXXX5698) for \$22,462.81. On the credit application, the applicant represented himself as M.A.R.² with a date of birth of xx/xx/1982 and social security number xxx-xx-4480. The applicant listed his address as 439 Andover Street, Lawrence, MA 01843, listed his occupation as the owner of “MRC Construction,” and stated that he made \$12,000 per month. He signed M.A.R.’s name to the application’s certification, which said, “By your signature below, you certify that you have completed this application to obtain credit, and that all information provided by you for this application is true, correct and complete.” During the sales process, the applicant presented Puerto Rico Driver’s license #9718354 as proof of identification. The document listed the name M.A.R. with date of birth xx/xx/1982 and displayed a photograph of a man matching the appearance of Andy MAZARA.³ After obtaining the Registry of Motor Vehicles photograph associated with the Massachusetts driver’s license of

¹ As discussed further below, surveillance video footage shows the individual at the Everett Dealership on October 12, 2018; however, all of the documentation relating to the vehicle purchase described below is dated October 13, 2018.

² The identity of victim M.A.R.C. is known to the government. In order, these initials represent the victim’s first name, middle name, paternal last name, and maternal last name. To protect the victim’s privacy, only the initials “M.A.R.C.” and “M.A.R.” are used in this affidavit to reflect the variations of the victim’s full name that were used by MAZARA.

³ The dealership made a copy or scan of this driver’s license and maintained it in its files pertaining to the transaction, which agents have reviewed.

MAZARA and comparing that photograph to the photograph on the fraudulent “M.A.R.” Puerto Rico driver’s license, agents determined that both photographs depict MAZARA.⁴ The applicant also provided the Everett Dealership with various documentation as proof of residence. He provided a residential lease in the name of M.A.R. at 439 Andover Street, Lawrence, MA, a National Grid bill in the name of M.A.R. with account number xxxx-x4838, and an Xfinity bill in the name of M.A.R. with account number xxxx-xx-xxx-xx7718X (last digit illegible) on page one, account number xxxx-xx-xxx-xx77188 on page two⁵, and a total amount due of \$722.53. On or about October 13, 2018, M.A.R. paid a \$500 deposit and took possession of the vehicle. No monthly payments were ever made on this vehicle loan.

8. Agents also obtained still images from surveillance footage from the Everett Dealership for the purchase of the above-mentioned Honda Accord from October 12, 2018. I have examined the still images from that footage and compared them to the driver’s license photo of MAZARA, and I determined that the surveillance footage depicts MAZARA communicating with an Everett Dealership employee.

9. The Honda Accord was subsequently entered into the National Crime Information Center (“NCIC”) as stolen and was recovered by DBFTF agents in Lawrence, MA. The vehicle was in the possession of an individual who admitted to agents that he knew that the vehicle was worth “\$30,000-\$40,000,” that he did not pay for it, and that he “knew something was up.” The individual was arrested for receiving stolen property in December 2019.

⁴ Additionally, MAZARA was arrested on April 2, 2020 while in possession of a fraudulent Maine driver’s license in another identity, which bore the exact same image as that which appeared on the M.A.R. Puerto Rico driver’s license described above.

⁵ When the fraudulent Xfinity bill was created, it appears that the creator overlooked the fact that the purported account numbers on pages one and two were different.

Confirmation of Valid Social Security Number; Identification of the Victim

10. The Social Security Administration (“SSA”) has confirmed that social security number xxx-xx-4480 is assigned to M.A.R., a United States citizen from Puerto Rico.

11. Law enforcement contacted the Puerto Rico Police Department to obtain the driver’s license of M.A.R. with social security number xxx-xx-4480. The Puerto Rico driver’s license for M.A.R. lists the name M.A.R.C., social security number xxx-xx-4480, and date of birth (xx-xx-1982), but a different driver’s license number (xxx0526) than the number on the Puerto Rico driver’s license presented by MAZARA at the Everett Dealership in October 2018. The driver’s license also displayed the photograph of a man who I believe to be the real M.A.R., who is different in appearance than the man depicted in the Puerto Rico driver’s license presented at the Everett Dealership.

RIVERA’s Aiding and Abetting the Fraudulent Purchase in the M.A.R. Identity

12. Agents received surveillance footage from a bank in Methuen, MA (the “Methuen Bank”) from October 4, 2018, the date that someone, using the M.A.R. identity opened a bank account at the branch. Still images from that footage depicted MAZARA in the Methuen Bank office, accompanied by RIVERA. Agents determined this was RIVERA based on a comparison to a photograph from when RIVERA was arrested by Methuen Police in January 2019.

13. The surveillance footage from the Everett Dealership during the October 12-13, 2018 purchase described above depicts what appears to be RIVERA in the background as MAZARA communicates with a dealership employee. Additionally, as detailed further below, agents seized RIVERA’s cell phone, and GPS location data saved in that phone place RIVERA’s cell phone at the Everett Dealership on October 12, 2018.

14. As described further below, on January 17, 2019, Methuen PD located a stolen 2018 Jeep Grand Cherokee that had been fraudulently purchased in Newton three days prior. RIVERA was in the driver's seat and was arrested for operation of a stolen motor vehicle.⁶ During an inventory search of the car, law enforcement located a sleeve of 500 blank ID cards, print ribbon, and retransfer film – items that I know, based on my training and experience, can be used to manufacture fraudulent ID cards. Also in the car, among other items, was a black iPhone.

15. On January 15, 2020, now-Chief U.S. Magistrate Judge M. Page Kelley signed a search and seizure warrant, 20-MJ-6003-MPK, for the black iPhone (Model A1778) that had been seized from the stolen 2018 Jeep Grand Cherokee. After a thorough search of the phone, DBFTF agents determined that the phone belonged to RIVERA based on communications with family members in which they called RIVERA by name, “selfie” photographs RIVERA sent to others, which depict RIVERA, and that the phone was frequently in the area of Kingston Street, Lawrence, MA (RIVERA and his girlfriend previously resided at 7 Kingston Street). In the phone, the owner's name was listed as “\$ ACE BUGGY \$” with an associated email address of “elmasloco24@icloud.com.” The phone contained a substantial amount of evidence which revealed that RIVERA played a role in obtaining stolen identities and producing false documents to be used for fraudulent vehicle purchases. Relevant here, on RIVERA's iPhone, DBFTF agents located a PDF version of an Xfinity bill with account number xxxx-xx-xxx-xx77188; an image of a fraudulent Puerto Rico driver's license bearing MAZARA's photograph and M.A.R.'s name, that appears the same as the document MAZARA presented at the Everett

⁶ As of the date of this affidavit, RIVERA's case is still pending. At the time of his arrest, he presented a fraudulent New Jersey driver's license in the name of L.K.R. and claimed that he was waiting for his girlfriend, Arialka MOYA, to get blood work done nearby. He was ultimately charged with providing a false address with intent to hinder police.

Dealership; an image of a social security card in the name of M.A.R.; and an identification card-style photograph of MAZARA that appears to be the same image on the fraudulent Puerto Rico driver's license that MAZARA presented at the Everett Dealership.

Fraudulent Vehicle Purchases in Arlington by Jose IRIZARRY

16. On or about December 7, 2018, a man later determined to be Jose IRIZARRY appeared in person at a car dealership in Arlington, Massachusetts (the "Arlington Dealership") and provided personal identifying information on two credit applications: one to purchase a 2018 Honda XR650L motorcycle (VIN: XXXXXXXXXXXXXXX0202) for \$9,165.99 with a \$431.19 down payment, and one to purchase a 2018 Honda XR650LJ motorcycle (VIN: XXXXXXXXXXXXXXX0967) for \$9,165.99 with \$431.19 down payment. On the credit applications, the applicant represented himself to be A.R.⁷ with a date of birth of xx/xx/1966 and social security number xxx-xx-0078. The applicant listed his address as 318 Nesmith Street, Apt. 12, Lowell, MA, listed his occupation as the owner of "Ruiz Construction," and stated that he earned \$19,166.67 per month on one application, and \$230,000 annually on the second application. On each application, he signed A.R.'s name to the application's certification, which said, "You promise that the information stated in this consumer loan application is true and correct to the best of your knowledge. You understand that it is a crime to willfully and deliberately provide incomplete or incorrect information to obtain credit." In connection with these purchases, the applicant presented Puerto Rico Driver's license #9672605 as proof of identification. The document listed the name A.O.R. with date of birth xx/xx/1966 and

⁷ The identity of victim A.O.R.M. is known to the government. In order, these initials represent the victim's first name, middle name, paternal last name, and maternal last name. To protect the victim's privacy, only the initials "A.O.R.M.," "A.O.R.," and "A.R." are used in this affidavit to reflect the variations of the victim's full name that were used by IRIZARRY.

displayed a photograph of a man matching the appearance of Jose Manuel IRIZARRY.⁸ After obtaining a booking photograph of IRIZARRY and comparing that photograph to the photograph on the fraudulent A.O.R. Puerto Rico driver's license, agents determined that both photographs depict IRIZARRY. The loans were approved, and the applicant took possession of the motorcycles (picking them up with his nephew). No monthly payments were ever made for these motorcycle loans.

17. According to a manager with the Arlington Dealership, it is "standard practice" to verify that a person to whom they are selling a motorcycle looks like the person on the photo identification that is presented during the sales process. Moreover, within RIVERA's black iPhone, DBFTF agents located three pictures of the two motorcycles purchased at the Arlington Dealership, and in one of the pictures Joshua CRUZ – a co-conspirator of RIVERA and IRIZARRY's, discussed further below – is depicted standing in front of both motorcycles.

Confirmation of Valid Social Security Number; Identification of the Victim

18. The Social Security Administration ("SSA") has confirmed that social security number xxx-xx-0078 is assigned to A.O.R., a United States citizen from Puerto Rico.

19. Law enforcement contacted the Puerto Rico Police Department to obtain the driver's license of A.O.R., with social security number xxx-xx-0078. The Puerto Rican driver's license for A.O.R. lists the name A.O.R.M. and social security number xxx-xx-0078, but a different date of birth (xx-xx-1963) and driver's license number (xxx4021) than that which was presented by the applicant at the Arlington Dealership in December 2018. The driver's license also displayed the photograph of a man who I believe to be the real A.O.R., who is different in

⁸ The dealership made a copy or scan of this driver's license and maintained it in its files pertaining to the transaction, which agents have reviewed.

appearance than the man depicted in the Puerto Rico driver's license presented at the Arlington Dealership (*i.e.*, IRIZARRY).

RIVERA's Aiding and Abetting, and Use of Wires to Facilitate, the Fraudulent Purchases in the A.O.R. Identity

20. On Rivera's iPhone, the search and seizure of which is described above, DBFTF agents located a signed social security card in the name of A.O.R. with a date stamp of 04/21/2011; a photograph of the Puerto Rico driver's license #9672605 in A.O.R.'s identity and bearing IRIZARRY's photo; a PDF version of a residential lease for A.O.R.; a fraudulent Xfinity bill in the name of A.O.R. with account number xxxx-xx-xxx-xx77188 and an amount due totaling \$722.53; and a PDF version of a bill of sale for the Honda XR650L that was fraudulently purchased on December 7, 2018.

21. Within the Arlington Dealership packet provided to DBFTF agents relating to the two motorcycle purchases, agents located several documents the applicant purporting to be A.O.R. presented to the dealership as proof of identity, income, and residence. These documents include the fraudulent Puerto Rico Driver's license #9672605, an Xfinity bill in the name of A.O.R. with account number xxxx-xx-xxx-xx7188 and with an amount due totaling \$722.53, a signed social security card in the name of A.O.R. with a date stamp of 04/21/2011, and a fraudulent U.S. Individual Income Tax Return Form 1040 in the name of A.O.R. with social security number xxx-xx-0078. All documents that were discovered in both RIVERA's phone and the Arlington Dealership packet appear to be the same.

22. On November 26, 2018, at approximately 4:10:24 PM (UTC-5) – less than two weeks before the fraudulent purchase of the Honda XR650L and XR650LJ – using the black iPhone described above, an email was sent over the internet from elmasloco24@icloud.com to staples@printme.com. The email, entitled “A.O.R.pdf,” contained the PDF attachment of the

above-described lease in the name of A.O.R. At approximately 4:11:29 PM (UTC-5), RIVERA received an email from no-reply@printme.com that stated, “Thank you for your online submission to Staples. Your document is ready for printing at any Staples store. It’s easy to retrieve your documents: Go to a self-serve printer in any Staples store to print your document Click on the Print option and select Print from Email Enter your personal release code or scan the barcode below Follow the on-screen instructions - it’s that easy! Release code: D1823FAC Release code will expire in 24 hours. List of document(s): A.O.R.pdf.”

23. On December 18, 2018, at approximately 10:12:15 AM (UTC-5) – 11 days after the fraudulent purchase of the Honda XR650L – using the black iPhone described above, an email was sent over the internet from elmasloco24@icloud.com to staples@printme.com. The email, entitled “Bill of Sale 16”, contained the PDF attachment of the above-described bill of sale in the name of A.O.R., for a Honda XR650L with VIN XXXXXXXXXXXXXXX0202. At approximately 10:12:29 AM (UTC-5), RIVERA received an email from no-reply@printme.com that stated, “Thank you for your online submission to Staples. Your document is ready for printing at any Staples store. It’s easy to retrieve your documents: Go to a self-serve printer in any Staples store to print your document Click on the Print option and select Print from Email Enter your personal release code or scan the barcode below Follow the on-screen instructions - it’s that easy! Release code: ED6A3BC8 Release code will expire in 24 hours. List of document(s): Bill of Sale 16.pdf.” The email sent from elmasloco24@icloud.com was associated with IP Address 17.142.180.58 which geolocates to Cupertino, CA. The email received by Staples was processed through AWS data centers in Northern VA. The documents were downloaded from a Staples store in North Andover, MA.

Fraudulent Vehicle Purchases in Newton and Brockton by Joshua CRUZ

24. On or about January 14, 2019, a man later determined to be Joshua CRUZ appeared in person at a car dealership in Newton, Massachusetts (the “Newton Dealership”) and provided personal identifying information on a credit application in an attempt to purchase a 2018 Jeep Grand Cherokee Summit (VIN: XXXXXXXXXXXXXXX4984) for \$53,249.06 with 100% financing. On the credit application, the applicant represented himself as E.J.M.⁹ with a date of birth of xx/xx/1979 and social security number xxx-xx-8598. The applicant listed his address as 3682 N Main Street, Apt. 10, Fall River, MA, listed his occupation as the owner of “Mendez Plumbing,” and stated he made \$216,000 per year. He signed the application’s certification, which said, “You certify that the information on the application and in any other application submitted to us, is true and complete. You understand that false statements may subject you to criminal penalties.” During the attempted purchase, the man presented Puerto Rico Driver’s license #8593216 as proof of identification. The document listed the name E.J.M.C. with date of birth xx/xx/1979 and displayed a photograph of a man matching the appearance of Joshua CRUZ.¹⁰ After obtaining the Massachusetts driver’s license of CRUZ and comparing that photograph to the photograph on the fraudulent Puerto Rico driver’s license, agents determined that both photographs depict CRUZ.

25. At the time, the dealership believed that the applicant had provided the proper documentation necessary to purchase the vehicle and therefore sold him a silver 2018 Jeep Grand Cherokee Summit for a total cost of \$53,249.06. The applicant obtained financing in

⁹ The identity of victim E.J.M.C. is known to the government. In order, these initials represent the victim’s first name, middle name, paternal last name, and maternal last name. To protect the victim’s privacy, only the initials “E.J.M.C.” and “E.J.M.” are used in this affidavit to reflect the variations of the victim’s full name that were used by CRUZ.

¹⁰ The dealership made a copy or scan of this driver’s license and maintained it in its files pertaining to the transaction, which agents have reviewed.

E.J.M.'s identity and paid no down payment. He picked up the vehicle on about January 15, 2019.

26. On January 16, 2019, CRUZ went to a car dealership in Brockton, MA (the "Brockton Dealership") and attempted to purchase a 2019 Jeep Grand Cherokee for a total of \$64,879.34. CRUZ presented Puerto Rico driver's license #8593216, social security card xxx-xx-8598, a National Grid bill, and an Xfinity bill, all in the name of E.J.M.C. After learning that an individual using the E.J.M.C. identity had fraudulently purchased a vehicle the prior day, the dealership contacted Brockton police, and CRUZ was arrested. Police found in his possession the fraudulent E.J.M.C. Puerto Rico driver's license described above.

27. The 2018 Jeep Grand Cherokee that had been purchased on January 14 was subsequently entered in to NCIC as stolen and was recovered by police officers in Methuen, MA on January 17, 2019. On that date, police found the vehicle with RIVERA in the driver's seat. RIVERA presented a New Jersey license in the name of "Luis Kianes Rivera." During the booking process, the individual's fingerprints came back to RIVERA. Located in the recovered Jeep Grand Cherokee was a box containing materials that can be used to fabricate identification cards. The fraudulent New Jersey license and identification materials were seized by the Methuen police department.

Confirmation of Valid Social Security Number; Identification of the Victim

28. The Social Security Administration ("SSA") has confirmed that social security number xxx-xx-8598 is assigned to E.J.M.C., a United States citizen from Puerto Rico.

29. Law enforcement contacted the Puerto Rico Police Department to obtain the driver's license of E.J.M.C., with social security number xxx-xx-8598. The Puerto Rico driver's license for E.J.M.C. lists the name E.J.M.C. and social security number xxx-xx-8598, but a

different date of birth (xx-xx-1979) and driver's license number (xxx9114) than that which was presented by CRUZ at the Newton Dealership in January 2019. The driver's license also displayed the photograph of a man who I believe to be the real E.J.M.C., who is different in appearance than the man depicted in the Puerto Rico driver's license presented at the Newton Dealership (*i.e.*, CRUZ).

RIVERA's Aiding and Abetting, and Use of Wires to Facilitate, the Fraudulent Purchases in the E.J.M.C. Identity

30. On Rivera's iPhone, the seizure and search of which is described above, DBFTF agents located a PDF version of a residential lease for E.J.M.C., as well as an identification card-style photograph of CRUZ that appears to be the same image on the fraudulent "E.J.M.C." Puerto Rico driver's license that was presented at the Newton Dealership by CRUZ. The address on the lease was 25 Ward Street, Apt. 1, Waterbury, CT.

31. On January 7, 2019, at approximately 6:56:34 AM (UTC-5), using the black iPhone described above, an email was sent over the internet from elmasloco24@icloud.com to staples@printme.com. The email contained a PDF attachment of the above-described lease in the name of E.J.M.C. with an address of 25 Ward Street, Apt. 1, Waterbury, CT. At approximately 6:56:48 AM (UTC-5), RIVERA received an email from no-reply@printme.com that stated, "Thank you for your online submission to Staples. Your document is ready for printing at any Staples store. It's easy to retrieve your documents: Go to a self-serve printer in any Staples store to print your document Click on the Print option and select Print from Email Enter your personal release code or scan the barcode below Follow the on-screen instructions - it's that easy! Release code: C8A4F1D9 Release code will expire in 24 hours." The email sent from elmasloco24@icloud.com was associated with IP Address 17.142.180.58 which geolocates

to Cupertino, CA. The email received by Staples was processed through AWS data centers in Northern VA. These documents were downloaded from a Staples store in Waterbury, CT.

32. On October 21, 2019, now-Chief U.S. Magistrate Judge M. Page Kelley signed a search and seizure warrant, 19-MJ-6507-MPK, for two Alcatel smartphones (IMEI # 015026002920476 and IMEI # 015026002896080) that were seized from CRUZ when he was arrested in Brockton, MA. Relevant here, CRUZ's phone contained a WhatsApp conversation between CRUZ and “\$ ACE \$” (RIVERA)¹¹ about the E.J.M.C. stolen identity and its use in the fraudulent vehicle purchase at the Newton Dealership. The following is a summary of the conversation that took place between January 5, 2019 and approximately January 14, 2019:

1	January 5, 2019	RIVERA	E.J.M.C. 25 Ward St. Apt. 1 Waterbury, CT, Monthly Rent: \$950 Been in Residence 5Y 4M DOB: xx/xx/1979 Age: 40 SSN: xxx-xx-8598 Email: mendezplumbing79@gmail.com Phone #: (860) 995-6848 Business Name: Mendez Plumbing Been in Business: 5Y 7M Annual Income: \$216,000 Monthly Income: \$18,000
2	January 7, 2019	RIVERA	<i>[Sends photo of Puerto Rico driver's license bearing CRUZ's photograph and social security card]</i>
3	January 9, 2019	CRUZ	The address on my info sucks I just spun them tho cause my address isn't there we googled it and it's a big parking so I spun them tho and convinced the that there was a house built in what was one time a backyard and numbered it 25 that it only been 4 yes [years] so the took it as 23 instead of 25
4	January 9, 2019	RIVERA	Ok
5	January 15, 2019	CRUZ	VIN# XXXXXXXXXXXXXXX4984, Fax# 6174542909, Email: mshaaban@mcovernaut.com
6	January 15, 2019	RIVERA	I'll get it done right now

¹¹ Investigation has revealed that RIVERA goes by the nickname or alias “Ace.” On August 31, 2018, an email was sent from elmasloco24@icloud.com (RIVERA’s known email address) to staples@printme.com and the subject line read, “Ace lease.” The email contained a PDF attachment of a residential lease with Alvin N Rivera as the leaseholder. RIVERA is also referred to as “Ace” in conversations within his iPhone.

7	January 15, 2019	CRUZ	U wanna talk to this guy directly cause he saying u don't even know what he needs do how u gonna idk bro idk. So we can all be on the same page
8	January 15, 2019	RIVERA	Who he think I am
9	January 15, 2019	CRUZ	He thinks ur the one who handles my insurance

Based on my review of the complete version of the excerpted conversation above, as well as my training and experience, I believe that RIVERA provided CRUZ with biographical details to use with the E.J.M.C. stolen identity and aided him in fraudulently purchasing the 2018 Jeep Grand Cherokee at the Newton Dealership and in attempting to purchase the 2019 Jeep Grand Cherokee at the Brockton Dealership. CRUZ used almost all the information in the excerpted conversation above to fill out the credit application that he submitted at the Newton Dealership in order to obtain financing.

33. This investigation has revealed that RIVERA provided other associates with stolen biographical data to use when purchasing vehicles. For example, within RIVERA's iPhone, DBFTF agents identified a WhatsApp conversation between RIVERA and Arialka MOYA, who is a subject of this investigation, that shows RIVERA providing such information. The following is a summary of the conversation that took place between December 14, 2018 and January 9, 2019:

1	RIVERA	Height: Weight: Eye Color: Hair Color:
2	MOYA	5'7" 195 Brown Brown
3	RIVERA	Gm Ari listen I am going to need that pic of u as soon as possible. If you need instructions on how I need that pic of u just ask
4	MOYA	Gm. Ok I'll do that now

5	RIVERA	I'm going to send u an example of how you need to have someone take the pics of you to send me. Take a few close up and at a lil distance shoulders up [attaches photograph of Andy MAZARA, a target of this investigation]
6	RIVERA	Look I'm working on your profiles like I told you I would [attaches photograph of L.A.P.N. Puerto Rico driver's license on a computer screen and a close up of two driver's licenses depicting MOYA in two separate identities] ¹²
7	MOYA	I hate that picture lol but thank you
8	RIVERA	L.A.P.N. 458 S 19 th St. Newark, NJ, Monthly Rent: \$950 Been in Residence 5Y 8M DOB: xx/xx/1980 Age: 38 SSN: xxx-xx-8077 Email: paganbeautysupply@gmail.com Phone #: (551) 689-0889 Business Name: Pagan Beauty Supply Been in Business: 5Y 7M Annual Income: \$215,000 Monthly Income: \$17,900 [also sends second identity information]
9	RIVERA	Hun those are your two profiles so you can start studying
10	MOYA	And kk I'll study that

Probable Cause to Search for Evidence of Target Offenses at Target Location

34. Based on the investigation to date, including the information summarized above, there is probable cause to believe that RIVERA has used false identification documents himself, and has been involved in making or otherwise procuring false identification documents for co-conspirators to use in opening bank accounts, obtaining credit cards, and obtaining loans to fraudulently purchase vehicles.

35. Based on the investigation to date, including the information summarized below, there is probable cause to believe that RIVERA lives at, and/or conducts his fraudulent business

¹² It appears that these were not legitimate driver's licenses but, rather, were counterfeit/fraudulent documents.

from, 15 Brockton Avenue, Haverhill, MA (the Target Location).¹³

36. According to the Haverhill Assessor's Office, 15-17 Brockton Ave, Haverhill, MA is classified as a two-family home.

37. On March 12, 2020, at approximately 9:36 am, while conducting physical surveillance of RIVERA and his associates, DBFTF agents observed a red Mazda CX7 bearing MA registration plates 3CFR51, exit Joy Terrace in Methuen, MA, and travel to the Days Inn hotel located at 129 Pelham Street, Methuen, MA. The Mazda was operated by a heavyset female wearing a leopard print shirt, subsequently identified as Neida LOPEZ, who picked up a bearded subject subsequently identified as MAZARA. After departing the Days Inn, the Mazda traveled to Brockton Avenue in Haverhill, MA, and picked up a short, heavyset male who was waiting on the street, subsequently identified as RIVERA.

38. On March 17, 2020, DBFTF agents conducted physical surveillance of RIVERA and his associates and observed RIVERA and an unknown male ("UM1") getting dropped off by the same red Mazda CX7 in the area of Lawrence Street, Haverhill, MA, not far from Brockton Avenue. At approximately 1:50 PM, surveillance units observed RIVERA and UM1 enter the building located at 15 Brockton Avenue, Haverhill, MA.

39. Surveillance of 15 Brockton Avenue, Haverhill, MA from March 2020 through September 3, 2020 showed RIVERA coming and going from that address on a regular basis – *i.e.*, more than 20 times.

40. During RIVERA's arrest on January 17, 2019 in Methuen, MA, RIVERA informed officers that his girlfriend, Person 1, would pick up his belongings. Surveillance of 15

¹³ RIVERA is currently on supervised release out of the United States District Court for the District of Massachusetts. He provided an address of 580 Hicks Street 3rd Floor, Fall River, MA, to U.S. Probation. However, based on the information described below, agents do not believe that is his primary residence.

Brockton Avenue from March 2020 through July 17, 2020 showed Person 1 coming and going on a regular basis.

41. Person 1 receives mail at 15 Brockton Avenue, Haverhill, MA.

42. On May 19, 2020, a woman appeared in person at a car dealership in Hooksett, NH and used a fraudulent Puerto Rico driver's license to purchase a 2009 silver Honda Accord. At the bottom of the sales application, there were hand-written notes which read, "Fedex: 15 Brockton Ave, Haverhill, MA 01830" and "M.C.,¹⁴ 860-382-6853." That phone number is known to be used by RIVERA. Additionally, the silver 2009 Honda Accord has been parked in the driveway of 15 Brockton Avenue, Haverhill, MA on a regular basis since the date of purchase, including most recently on August 20, 2020.

43. On September 8, 2020, Haverhill police conducted a ruse at the Target Location. Police knocked on the front door of the Target Location, and Person 1 answered the door. A man matching the appearance of RIVERA was standing inside in an entry-way area, which appeared to lead to the living area and the rest of the residence.

44. I know, based on my training and experience, that:

- a. Individuals often keep identification documents and financial records and other evidence of identity for long periods – sometimes years – and tend to retain such documents even when they depart a given residence. Such documents include driver's licenses, social security cards, bank cards, credit cards, bank records, and credit card statements.
- b. Individuals often keep identification documents and financial records in their residence, in part to ensure the security of these documents and in

¹⁴ M.C. might be a victim of identity theft and therefore only the initials M.C. are used in this affidavit.

part to allow for access to these documents when needed.

- c. In addition, it is common for those who use other persons' identities without authorization to maintain fraudulently obtained identification documents in secure locations within their residence to conceal them from law enforcement authorities;
- d. It is common for individuals who use fraudulently obtained identification documents to retain those documents for substantial periods of time so that they can continue to use the fraudulently obtained identities;
- e. Individuals involved in making false identification documents often use computers, cell phones, printers, and similar equipment to create the false identification documents. This equipment is often stored in the individual's home. This equipment is expensive and durable, and can be stored and used for years; and
- f. Based on my experience and training, I also know that individuals who make purchases of goods and services often retain their receipts and invoices in their residence.

45. I also know, based on my training and experience:

- a. Individuals frequently use computer equipment to carry out, communicate about, and store records regarding their daily activities. These tasks are frequently accomplished through sending and receiving e-mail, instant messages, and other forms of phone or internet based messages; scheduling activities; keeping a calendar of activities; arranging travel; purchasing items; searching for information including information

regarding travel and activities; arranging for travel, accessing personal accounts including banking information; paying for items; and creating, storing, and transferring images, videos, and other records of their movements and activities.

- b. Individuals involved in criminal activity, to include the planning and execution of identity theft schemes, communicate with each other through the use of cellular telephones. Additionally, I am also aware that individuals involved in criminal activity, to include the planning and execution of identity theft schemes, communicate using social media networking sites like Facebook, Snapchat, WhatsApp, etc. which can be accessed through cellular telephones.
- c. I know that many smartphones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.
- d. I am aware that individuals commonly store records of the type described in Attachment B in mobile phones, computer hardware, computer software, and storage media.
- e. I know that data can often be recovered months or even years after it has

been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

- i. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their electronic equipment, they can easily transfer the data from their old device to a new one.
- ii. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a device, the data contained in the file often does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, the device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- iii. Wholly apart from user-generated files, electronic storage media often contains electronic evidence of how the device has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but users typically do not erase or delete this evidence because special software is typically required for that task.

iv. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

Conclusion

46. Based on the foregoing, I submit that there is probable cause to believe that (1) on or about October 13, 2018, December 7, 2018, and January 14, 2019, Alvin RIVERA (a) falsely represented, with intent to deceive and for any purpose, a number to be the social security account number assigned by the Commissioner of Social Security to another person, when in fact such number is not the social security account number assigned by the Commissioner of Social Security to such other person, and aided and abetted the same, all in violation of 42 U.S.C. § 408(a)(7)(B) and 18 U.S.C. § 2; and (b) knowingly transferred, possessed and used, during and in relation to any felony violation enumerated in 18 U.S.C. 1028A(c), and without lawful authority, a means of identification of another person, and aided and abetted the same, all in violation of 18 U.S.C. § 1028A and 18 U.S.C. § 2; and that (2) on or about December 18, 2018, and January 7, 2019, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing the scheme to defraud, to wit, stolen identity information to Staples in violation of 18 U.S.C. § 1343.

47. Based on the forgoing, I have probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as described in Attachment B, are located in the premises described in Attachment A.

Signed under the pains and penalties of perjury this 9th day of September, 2020.

/s/ Timothy Taber

Timothy Taber
Special Agent
Homeland Security Investigations

Subscribed and sworn to via telephone in accordance with Federal Rule of Criminal Procedure 4.1 this 9th day of September, 2020.


HONORABLE M. PAGE KELLEY
CHIEF UNITED STATES MAGISTRATE JUDGE
DISTRICT OF MASSACHUSETTS



20-MJ-6560-MPK

ATTACHMENT A
Premises To Be Searched

The location to be searched is 15 Brockton Avenue, Haverhill, MA 01830, one of two marked addresses in a gray multifamily home, with the number 15 on the right-side column on the front steps. There are two front-door entrances to the building, one for 17 Brockton Avenue, which is located on the left, and one for 15 Brockton Avenue, which is located on the right. A photograph of the home is attached.

Front View of 15 Brockton Ave, Haverhill, MA



20-MJ-6560-MPK

ATTACHMENT B
Evidence to Be Searched for and Seized

Evidence, fruits, and instrumentalities of violations of 42 U.S.C. § 408(a)(7)(B),
18 U.S.C. § 1343, and 18 U.S.C. § 1028A, including but not limited to:

1. Any government-issued or apparently government-issued identification documents, notes, statements, and/or receipts that reference same;
2. Any fraudulent, stolen, or apparently fraudulent or stolen identification documents, as well as any records and communications relating to same, and any tangible items used to create or modify any identification documents;
3. Any fraudulent, stolen, or apparently fraudulent or stolen credit cards, bank cards, and records, communications, and other documents related to the same, and any tangible items used to create or modify any credit or bank cards;
4. Bank records and credit card records from January 1, 2018 to the date of execution of the warrant;
5. Records, communications, and other documents relating to the purchase or attempted purchase, financing, insuring, registration, titling, re-titling, and/or sale of any automobile and/or other vehicle, as well as funds relating to same;
6. Records, communications, and other documents relating to the movement, shipment, or export of any automobile and/or other vehicle, as well as funds relating to same;
7. Records, communications, and other documents relating to any alias or imposter identity used to purchase or attempt to purchase any automobile and/or other vehicle; identification documents, credit or bank cards, or other records in the

name(s) of such aliases; and/or any records relating to other accounts in the name(s) of such aliases;

8. Records relating to any purchase, sale, or other transaction conducted in any alias or imposter identity, or any account opened up under an alias or imposter identity;
9. Communications with any individual involved with committing and/or conspiring to commit any of the TARGET OFFENSES;
10. Communications with any individual who participated in the planning or execution of any purchase, sale, or other transaction conducted in any alias or imposter identity, or who participated in the opening or use of any account opened under an alias or imposter identity;
11. Receipts and other records relating to the expenditure of funds associated with any purchase, sale, or other transaction conducted in any alias or imposter identity;
12. Records relating to any of the proceeds derived from any of the TARGET OFFENSES, including records showing the receipt, transfer, spending, or use of such proceeds;
13. Records and tangible objects relating to the ownership, occupancy, control, or use of the premises to be searched (such as utility bills, phone bills, bank statements, rent payments, insurance documentation, receipts, check registers, and correspondence);
14. Records and tangible objects relating to the ownership, control, or use of any vehicle, phone, or other device used in furtherance of any of the TARGET OFFENSES;
15. Bulk cash and high-value items believed to be the proceeds or fruits of fraudulent

credit card transactions or stolen car sales;

16. Tangible objects, and records related to such objects, capable of being used in the creation, production, and distribution of counterfeit identification documents, including: computers, laptop computers, printers, ink cartridges, printer paper, laminators, and cutting boards;
17. Cellular phones;
18. Any and all electronic media storage devices, including SIM cards, hard drives, USB drives, memory sticks, tablets, and external hard drives; and
19. For any computer hardware, computer software, mobile phones, or storage media called for by this warrant or that might contain things otherwise called for by this warrant (“the computer equipment”)
 - a. Evidence of who used, owned, or controlled the computer equipment;
 - b. Evidence of the presence or absence of malicious software that would allow others to control the items, and evidence of the presence or absence of security software designed to detect malicious software;
 - c. Evidence of the attachment of other computer hardware or storage media;
 - d. Evidence of counter-forensic programs and associated data that are designed to eliminate data;
 - e. Evidence of when the computer equipment was used;
 - f. Passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and

g. Records and tangible objects pertaining to accounts held with companies providing internet access or remote storage.

20. All computer hardware, computer software, and storage media. Off-site searching of these items shall be limited to searching for the items described above.

DEFINITIONS

For the purpose of this warrant:

- A. “Computer equipment” means any computer hardware, computer software, mobile phone, storage media, and data.
- B. “Computer hardware” means any electronic device capable of data processing (such as a computer, smartphone, mobile phone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections}, and any security device, (such as electronic data security hardware and physical locks and keys).
- C. “Computer software” means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.
- D. “Storage media” means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- E. “Data” means all information stored on storage media of any form,

in any storage format and for any purpose.

F. “A record” is any communication, representation, information or data. A “record” may be comprised of letters, numbers, pictures, sounds or symbols.

RETURN OF SEIZED COMPUTER EQUIPMENT

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy’s authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system’s owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, or personally-identifying information of victims; or the fruits or instrumentalities of crime.

For purposes of authentication at trial, the Government is authorized to retain a digital copy of all computer equipment seized pursuant to this warrant for as long as is necessary for authentication purposes.